PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-261549
(43)Date of publication of application : 24.09.1999

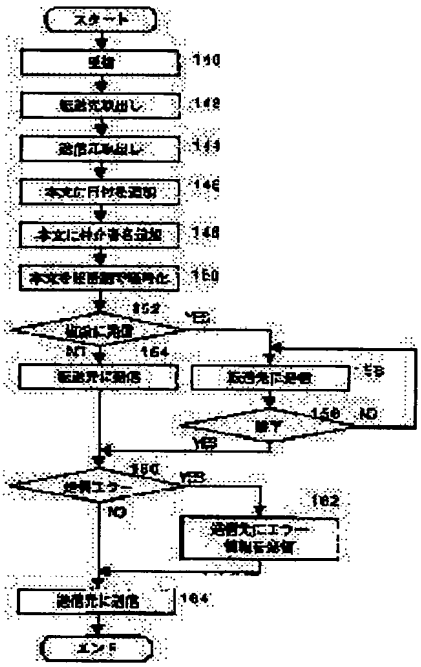
(51)Int.Cl. H04L 9/32
G06F 13/00
H04L 12/54
H04L 12/58

(21)Application number : 10-059485
(22)Date of filing : 11.03.1998

(71)Applicant : SHARP CORP
(72)Inventor : YOSHIDA HIROICHI

(54) CONTENT-CERTIFIED ELECTRONIC MAIL DEVICE, METHOD AND STORAGE MEDIUM FOR CONTENT-CERTIFIED ELECTRONIC MAIL PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a service that corresponds to content-certified mail in an electronic mail system.
SOLUTION: This content-certified electronic mail method includes an electronic mail receiving step (140) that receives an electronic mail and a content- certified transmitting step (142 to 158) which guarantees the identity of the originator of a received electronic mail, a receiving time and content and transmits the received electronic mail to the transfer destination of the received electronic mail. The content-certified transmitting step enciphers a received mail with the secret key of an operator of the electronic mail device (150) and can include a step that allows the operator of the electronic mail device to transmit the mail as an originator to the transfer destination included in the received mail. Preferably, it further includes a return step (164) in which a transmitter also returns an electronic mail that has the same content as the electronic mail sent to the transfer destination to the originator. Both a storage medium that stores a program to accomplish the same purpose and a device are open to the public.



LEGAL STATUS

[Date of request for examination] 12.01.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－261549

(43)公開日　平成11年(1999)９月24日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７１
Ｇ０６Ｆ	13/00	３５１	Ｇ０６Ｆ	13/00	３５１Ｇ
Ｈ０４Ｌ	12/54		Ｈ０４Ｌ	9/00	６７３Ｂ
	12/58			11/20	１０１Ｂ

審査請求　未請求　請求項の数11　ＯＬ　（全 11 頁）

(21)出願番号　特願平10－59485

(22)出願日　平成10年(1998)３月11日

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号

(72)発明者　吉田　広市
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内

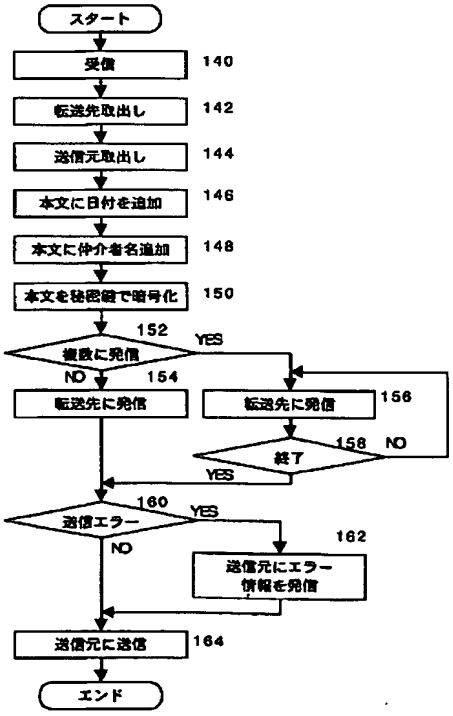
(74)代理人　弁理士　深見　久郎

(54)【発明の名称】　内容証明電子メール装置および方法ならびに内容証明電子メールプログラムの記憶媒体

(57)【要約】

【課題】　内容証明郵便に相当するサービスを電子メールシステムで実現。

【解決手段】　内容証明電子メール方法は、電子メールを受信するための電子メール受信ステップ（１４０）と、受信した電子メールの発信者、受信時刻および内容の同一性を保証して、受信した電子メールを、受信した電子メールの転送先に送信する内容証明送信ステップ（１４２～１５８）とを含む。内容証明送信ステップは、受信したメールを当該内容証明電子メール装置の運用者の秘密鍵で暗号化し（１５０）、受信したメールに含まれる転送先に当該内容証明電子メール装置の運用者を発信者として送信するステップを含んでもよい。好ましくは、送信装置が転送先に送信する電子メールと同じ内容の電子メールを発信者にも返信するための返信ステップ（１６４）をさらに含む。同様の目的を達成するためのプログラムを記憶した記憶媒体と、装置とも開示されている。



1

【特許請求の範囲】

【請求項１】　電子メールを受信するための電子メール受信手段と、

受信した電子メールの発信者、受信時刻および内容の同一性を保証して、前記受信した電子メールを、前記受信した電子メールの転送先に送信する内容証明送信手段とを含む、内容証明電子メール装置。

【請求項２】　前記内容証明送信手段は、

前記受信したメールを当該内容証明電子メール装置の運用者の秘密鍵で暗号化し、前記受信したメールに含まれる転送先に当該内容証明電子メール装置の運用者を発信者として送信するための送信手段を含む、請求項１に記載の内容証明電子メール装置。

【請求項３】　前記内容証明送信手段は、

前記受信した電子メールを当該内容証明電子メール装置の運用者の秘密鍵で暗号化し、前記受信した電子メールに含まれる転送先の全てに当該内容証明電子メール装置の運用者を発信者として送信するための送信手段を含む、請求項１に記載の内容証明電子メール装置。

【請求項４】　前記送信手段が転送先に送信する電子メールと同じ内容の電子メールを当該電子メールの発信者に返信するための返信手段をさらに含む、請求項２または請求項３に記載の内容証明電子メール装置。

【請求項５】　さらに、前記内容証明送信手段による転送先への電子メールの送信が失敗したことに応答して、前記受信したメールの発信者に対して電子メールの送信失敗に関する情報を送信するためのエラー情報送信手段を含む、請求項１に記載の内容証明電子メール装置。

【請求項６】　電子メールを受信する電子メール受信ステップと、

受信した電子メールの発信者、受信時刻および内容の同一性を保証して、前記受信した電子メールを、前記受信した電子メールの転送先に送信する内容証明送信ステップとを含む、内容証明電子メール方法。

【請求項７】　前記電子メール受信ステップは、

前記受信したメールを当該内容証明電子メール方法の運用者の秘密鍵で暗号化し、前記受信したメールに含まれる転送先に当該内容証明電子メール方法の運用者を発信者として送信するための送信ステップを含む、請求項６に記載の内容証明電子メール方法。

【請求項８】　前記内容証明送信ステップは、

前記受信した電子メールを当該内容証明電子メール装置の運用者の秘密鍵で暗号化し、前記受信した電子メールに含まれる転送先の全てに当該内容証明電子メール装置の運用者を発信者として送信する送信ステップを含む、請求項６に記載の内容証明電子メール方法。

【請求項９】　前記送信ステップが転送先に送信する電子メールと同じ内容の電子メールを当該電子メールの発信者に返信する返信ステップをさらに含む、請求項７または請求項８に記載の内容証明電子メール方法。

2

【請求項１０】　さらに、前記内容証明送信ステップによる転送先への電子メールの送信が失敗したことに応答して、前記受信したメールの発信者に対して電子メールの送信失敗に関する情報を送信するためのエラー情報送信ステップを含む、請求項６に記載の内容証明電子メール方法。

【請求項１１】　請求項６から請求項１０のいずれかに記載の内容証明電子メール方法を実現するプログラムを機械可読な形式で記録した、内容証明電子メールプログラムの記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は電子メールシステムに関し、特に、既存の郵便システムにおける内容証明郵便に類似した機能を提供することができる電子メールシステムに関する。

【０００２】

【従来の技術】ネットワークの普及にともなって、既存の郵便制度と別の電子メールシステムが広く使用されるようになっている。特に、インターネットの使用が広まることで、異なる組織に属する人でも、互いの組織がインターネットへの接続を行なってさえいれば、電子メールの授受が可能となってきたこと、および既存の郵便を利用するのと比較して電子メールははるかに手軽に利用できること、により、その利用は増加しつつある。

【０００３】一方で、インターネットでは、電子メールに限らず、配信データは複数のコンピュータを介して配送されるため、そのセキュリティに不安があるとされる。そのため、電子メール等を用いたトランザクションをいかに安全に指定された相手に配送するか、について近年多大な労力が払われている。

【０００４】それら労力のうちのかなりの部分が、特に最近のいわゆる「エレクトロニック・コマース」や電子マネーの実用化研究に関連して、情報の盗聴、改ざん、「なりすまし」などと呼ばれる不正行為を防止するための技術に払われている。

【０００５】それら技術のうちで、特に脚光を浴びているのがいわゆる暗号化技術である。なかでも、暗号化アルゴリズムが公開されている手法を用いることが、インターネット上で安心して使用できるアルゴリズムの一つの要件であるとされている。暗号化技術の概略の傾向については、「インターネット時代の暗号技術」（三好敏、日経エレクトロクニス、Ｎｏ．６５８，２２３頁以下）を参照されたい。

【０００６】そうした暗号化技術の一つに、公開鍵を用いたものがある。公開鍵暗号系には、暗号化する際に用いる鍵と、復号する際に用いる鍵との２つの鍵が使用される。この二つの鍵は互いに入れ替えても暗号化および復号化が可能である。

【０００７】この二つのうちの一つの鍵を公開し（公開

鍵）、他方の鍵を自分など一部の者だけが知っておく（秘密鍵）ようにする。以下、対となる公開鍵と秘密鍵とをまとめて暗号鍵データと呼ぶ。公開鍵は、公開鍵簿と呼ばれるリストに登録され、だれでも知ることができる。こうした暗号鍵データを使用することで、色々なことができる。

【０００８】例えば、図９を参照して、ある受信者の暗号鍵データ２１４が公開鍵２２０と秘密鍵２２２とを含むものとする。このとき、この受信者とは別の送信者の送信者装置２１０から当該受信者の装置２１２に対してインターネットを介して秘密の情報を送信するときは次のような処理を行なう。送信者装置２１０は、受信者の公開鍵２２０を用いて情報を暗号化する。インターネット２６を介してこの情報を受信した受信者装置２１２は、この情報を秘密鍵２２２を用いて復号化する。公開鍵２２０を用いて暗号化された情報は、秘密鍵２２２を用いなければ解読できない。したがって、秘密鍵２２２が人に知られない限り、インターネット２６上で情報が盗聴されたとしても直ちにその内容が知られる訳ではない。

【０００９】逆に図１０を参照して、送信者側の暗号鍵データ２３０を用いて、送信者の認証を行なうことができる。たとえば、送信者の暗号鍵データ２３０が秘密鍵２４０と公開鍵２４２とを含むものとする。秘密鍵２４０は送信者のみが知っている。公開鍵２４２は誰でも知ることができる。この場合、送信者装置２１０で送信情報を秘密鍵２４０を用いて暗号化し、暗号化された情報をインターネット２６を会して受信者装置２１２に送信する。受信者は、送信者の公開鍵２４２を用いてこの情報を復号化する。うまく復号化できたら、その情報は秘密鍵２４０によって暗号化されていたことが分かる。秘密鍵２４０を知っているのは正しい送信者のみであるから、これによりデータを送信してきた者がその送信者その人であることが分かる。

【００１０】

【発明が解決しようとする課題】このように、公開鍵方式を用いた暗号化により、ある程度の信頼性および安全性をもって情報を伝達することができる。しかし、電子メールシステムにおいては、このような暗号化のみによっては解決できない問題がある。

【００１１】その一つが、在来の郵便制度で提供されている書留や内容証明郵便（以下まとめて「内容証明郵便」と呼ぶ。）に相当する機能が、従来の電子メールシステムでは提供できなかったという問題である。この問題は、そうしたサービスを提供するためには発信者と受信者との間でこの間のメール送信の仲介を行なう者の存在が必要であるにもかかわらず、従来の電子メールシステムではそうした仲介者となるものがないこと、仮に仲介者となるものがいたとしても、電子メールでは電子データを容易に偽造したり改ざんしたりることができるため、書留や内容証明郵便に相当するサービスを提供すること自体が困難と考えられていたこと、による。またこうしたサービスを提供する上で、電子メールの内容をすべて一カ所に記憶しておいたりする手法が考えられないわけではないが、その場合には膨大な容量の外部記憶装置が必要となるという問題がある。さらに、複数の送信先に同一の内容の電子メールを発信する際に、そうした内容証明郵便に相当するサービスが提供できれば便利である。また、そうした内容証明郵便に相当する電子メールの発信の後、その内容が正しいことを確認できると好ましい。また、電子メールの送信にあたって、受信者のメールサーバが故障していたりすると、正常なメールの送信が行なわれない場合がある。この時も、メールの送信が正常に行なわれなかったことを知ることができればさらに好ましい。

【００１２】それ故に請求項１または請求項２に記載の発明の目的は、内容証明郵便に相当するサービスを電子メールシステムで実現できる内容証明電子メール装置を提供することである。

【００１３】請求項３に記載の発明の目的は、複数の宛先に対して同一内容の電子メールを発信する際に内容証明郵便に相当するサービスを電子メールシステムで実現できる内容証明電子メール装置を提供することである。

【００１４】請求項４に記載の発明の目的は、内容証明郵便に相当するサービスを電子メールシステムで実現でき、かつ送信された内容を確認できる内容証明電子メール装置を提供することである。

【００１５】請求項５に記載の発明の目的は、内容証明郵便に相当するサービスを電子メールシステムで実現でき、かつ送信が失敗したことを発信者に通知できる内容証明電子メール装置を提供することである。

【００１６】請求項６または請求項７に記載の発明の目的は、内容証明郵便に相当するサービスを電子メールシステムで実現できる内容証明電子メール方法を提供することである。

【００１７】請求項８に記載の発明の目的は、複数の宛先に対して同一内容の電子メールを発信する際に内容証明郵便に相当するサービスを電子メールシステムで実現できる内容証明電子メール方法を提供することである。

【００１８】請求項９に記載の発明の目的は、内容証明郵便に相当するサービスを電子メールシステムで実現でき、かつ送信された内容を確認できる内容証明電子メール方法を提供することである。

【００１９】請求項１０に記載の発明の目的は、内容証明郵便に相当するサービスを電子メールシステムで実現でき、かつ送信が失敗したことを発信者に通知できる内容証明電子メール方法を提供することである。

【００２０】請求項１１に記載の発明の目的は、請求項６～請求項１０に記載の、内容証明郵便に相当するサービスを電子メールシステムで実現できる内容証明電子メ

ール方法を実現する内容証明電子メールプログラムの記憶媒体を提供することである。

【００２１】

【課題を解決するための手段】請求項１に記載の発明にかかる内容証明電子メール装置は、電子メールを受信するための電子メール受信手段と、受信した電子メールの発信者、受信時刻および内容の同一性を保証して、受信した電子メールを、受信した電子メールの転送先に送信する内容証明送信手段とを含む。

【００２２】受信した電子メールの発信者と、受信時刻と、その内容との同一性を保証して転送先に送信する内容証明送信手段により、発信者とは異なる第三者によって、その電子メールの内容証明が提供される。

【００２３】請求項２に記載の発明にかかる内容証明電子メール装置は、請求項１に記載の発明の構成に加えて、内容証明送信手段は、受信したメールを当該内容証明電子メール装置の運用者の秘密鍵で暗号化し、受信したメールに含まれる転送先に当該内容証明電子メール装置の運用者を発信者として送信するための送信手段を含む。

【００２４】内容証明電子メール装置の運用者の秘密鍵は、当該運用者にしか知られない。したがってその運用者から発信された電子メールを当該運用者の公開鍵で復号化できれば、その電子メールは確かに当該運用者から送信されたものであることが分かる。したがってその電子メールの内容証明の信ぴょう性を高めることができる。

【００２５】請求項３に記載の発明にかかる内容証明電子メール装置は、請求項１に記載の発明の構成に加えて、内容証明送信手段は、受信した電子メールを当該内容証明電子メール装置の運用者の秘密鍵で暗号化し、受信した電子メールに含まれる転送先の全てに当該内容証明電子メール装置の運用者を発信者として送信するための送信手段を含む。

【００２６】内容証明電子メール装置が、複数の転送先のすべてに電子メールを送信するので、発信者は、１通の電子メールと、必要な転送先の宛名とを内容証明電子メール装置に対して発信すればよく、簡単に複数の相手に対して内容証明された電子メールを送ることができる。

【００２７】請求項４に記載の発明にかかる内容証明電子メール装置は、請求項２または請求項３に記載の発明の構成に加えて、送信手段が転送先に送信する電子メールと同じ内容の電子メールを当該電子メールの発信者に返信するための返信手段をさらに含む。

【００２８】転送先に送信されたのと同じ電子メールを発信者に対して送信することで、発信者は内容証明のメールが受信者に転送されたことを知ることができる。しかも返送される電子メールは内容証明電子メール装置の運用者の秘密鍵で暗号化されている。したがって当該電子メールが確かに内容証明電子メール装置から返送されたものであることが保証され、その電子メールを発信者が保持しておくことで、その内容証明を行なうことができる。またこれにより内容証明電子メール装置自体は、内容証明したメールのコピーを保持しておく必要がなくなり、大量の電子メールを処理したとしても、外部記憶装置などの資源が不足するおそれは少ない。

【００２９】請求項５に記載の発明にかかる内容証明電子メール装置は、請求項１に記載の発明の構成に加えてさらに、内容証明送信手段による転送先への電子メールの送信が失敗したことに応答して、受信したメールの発信者に対して電子メールの送信失敗に関する情報を送信するためのエラー情報送信手段を含む。

【００３０】内容証明のメールの送信に失敗したことが発信者に対して通知されるので、発信者は適切な対応をすることが可能になる。

【００３１】請求項６に記載の発明にかかる内容証明電子メール方法は、電子メールを受信する電子メール受信ステップと、受信した電子メールの発信者、受信時刻および内容の同一性を保証して、受信した電子メールを、受信した電子メールの転送先に送信する内容証明送信ステップとを含む。

【００３２】受信した電子メールの発信者と、受信時刻と、その内容との同一性を保証して転送先に送信する内容証明送信ステップにより、発信者とは異なる第三者によって、その電子メールの内容証明が提供される。

【００３３】請求項７に記載の発明にかかる内容証明電子メール方法は、請求項６に記載の発明の構成に加えて、電子メール受信ステップは、受信したメールを当該内容証明電子メール方法の運用者の秘密鍵で暗号化し、受信したメールに含まれる転送先に当該内容証明電子メール方法の運用者を発信者として送信するための送信ステップを含む。

【００３４】内容証明電子メール方法の運用者の秘密鍵は、当該運用者にしか知られない。したがってその運用者から発信された電子メールを当該運用者の公開鍵で復号化できれば、その電子メールは確かに当該運用者から送信されたものであることが分かる。したがってその電子メールの内容証明の信ぴょう性を高めることができる。

【００３５】請求項８に記載の発明にかかる内容証明電子メール方法は、請求項６に記載の発明の構成に加えて、内容証明送信ステップは、受信した電子メールを当該内容証明電子メール装置の運用者の秘密鍵で暗号化し、受信した電子メールに含まれる転送先の全てに当該内容証明電子メール装置の運用者を発信者として送信する送信ステップを含む。

【００３６】内容証明電子メール方法により、複数の転送先のすべてに電子メールが送信されるので、発信者は、１通の電子メールと、必要な転送先の宛名とを内容

証明電子メール方法の運用者に対して発信すればよく、簡単に複数の相手に対して内容証明された電子メールを送ることができる。

【００３７】請求項９に記載の発明にかかる内容証明電子メール方法は、請求項７または請求項８に記載の発明の構成に加えて、送信ステップが転送先に送信する電子メールと同じ内容の電子メールを当該電子メールの発信者に返信する返信ステップをさらに含む。

【００３８】転送先に送信されたのと同じ電子メールを発信者に対して送信することで、発信者は内容証明のメールが受信者に転送されたことを知ることができる。しかも返送される電子メールは内容証明電子メール方法の運用者の秘密鍵で暗号化されている。したがって当該電子メールが確かに内容証明電子メール方法の運用者から返送されたものであることが保証され、その電子メールを発信者が保持しておくことで、その内容証明を行なうことができる。またこれにより内容証明電子メール方法を運用する装置自体は、内容証明したメールのコピーを保持しておく必要がなくなり、大量の電子メールを処理したとしても、外部記憶装置などの資源が不足するおそれは少ない。

【００３９】請求項１０に記載の発明にかかる内容証明電子メール方法は、請求項６に記載の発明の構成に加えてさらに、内容証明送信ステップによる転送先への電子メールの送信が失敗したことに応答して、受信したメールの発信者に対して電子メールの送信失敗に関する情報を送信するためのエラー情報送信ステップを含む。

【００４０】内容証明のメールの送信に失敗したことが発信者に対して通知されるので、発信者は適切な対応をすることが可能になる。

【００４１】請求項１１に記載の発明にかかる内容証明電子メールプログラムの記憶媒体は、請求項６から請求項１０のいずれかに記載の内容証明電子メール方法を実現するプログラムを機械可読な形式で記録したものである。

【００４２】この記憶媒体に記憶されたプログラムをコンピュータに実行させることにより、請求項６から請求項１０に記載した発明と同様の効果を得ることができる。

【００４３】

【発明の実施の形態】図１を参照して、本願発明の一実施の形態の電子メールシステムは、互いにインターネット２６に接続された送信者装置２０および受信者装置２４に加えて、送信者装置２０から受信者装置２４への内容証明電子メールを仲介するための仲介者装置２２とを含む。本実施の形態では、送信者が、秘密鍵４０および公開鍵４２を含む暗号鍵データ３０を有し、仲介者が、秘密鍵４４および公開鍵４６を含む暗号鍵データ３２を有しているものとする。

【００４４】なお、送信者がこのように自分の暗号鍵データ３０を持っていることは仲介者装置２２による内容証明の処理にとっては関係なく、なくとも構わない。

【００４５】発信者装置２０は、全体を管理するための処理を行なうプログラムを実行するＣＰＵ５０と、文字を入力するための入力装置５２と、入力された情報を表示するための表示装置５４と、入力された文字を編集するための編集装置５６と、編集されたデータを送受信するための通信装置６０と、表示プログラム、編集プログラム、暗号化および復号化プログラムならびに各処理に使用されるデータが格納されるＲＡＭ６２と、表示プログラム、編集プログラム、暗号化および復号化プログラムなどを記録した記憶媒体６４等からプログラム、データなどを読み取り、ＲＡＭ６２に格納するための外部記憶装置５８とを含む。

【００４６】受信者装置２４も、送信者装置２０と同じ構成を有するので、ここではその詳細はくり返さない。

【００４７】図３を参照して、仲介者装置２２は、全体を管理するための処理を行なうプログラムを実行するＣＰＵ７０と、電子メールを受信するための受信装置７２と、電子メールを送信するための送信装置８０と、電子メールを暗号化するための暗号装置７４と、送信された電子メールを一時的に保持するためのデータバッファ８２と、電子メールがこの仲介者装置２２を通過した時間をスタンプするための時計７６と、発信者情報と受信者情報とを保存するためのバッファ８４と、暗号装置７４を実現するためのプログラム８８を記憶するためのＲＡＭ８６と、当該暗号化プログラムを機械可読な形式で記憶した記憶媒体９０から暗号化プログラムを読み出し、ＲＡＭ８６に格納するための外部記憶装置７８とを含む。

【００４８】データの流れは以下のようになる。図４を参照して、送信者装置２０では、送信内容１００を自己の秘密鍵４０を用いて暗号化する。暗号化した送信内容１０２を電子メールで仲介者装置２２に宛てて送る。このとき、真の送信先（受信者）を転送先として電子メール中で指定しておく。

【００４９】仲介者装置２２は、受信したメールのデータにそのメールの受信日付および仲介者の名称を付加し、さらに自己の秘密鍵４４を用いて暗号化する。仲介者装置２２は、このようにさらに暗号化した送信内容１０４を、指定された転送先である受信者装置２４に宛てて電子メールで送信する。受信者装置２４は、仲介者装置２２から電子メールを受け取ると、仲介者装置２２の公開鍵４６を用いて復号化する。公開鍵４６で電子メールを復号化できれば、この電子メールが仲介者装置２２から送られてきたものであることが確認できる。この場合、復号化することにより発信者装置２０で暗号化された送信内容１０６が得られるので、必要であればこの送信内容をさらに復号化すれば必要な情報が得られる。

【００５０】また、仲介者装置２２は、受信者装置２４

に宛てて送信した送信内容１０４と同じ送信内容１０８を電子メールで送信者装置２０に宛てて送信する。発信者装置２０は、この電子メールを仲介者２２の公開鍵を用いて復号化して、自己が暗号化した送信内容１１０を得る。この送信内容をさらに復号化して得られた送信内容１１２が、最初の送信内容１００と等しければ、正しい内容の電子メールが受信者装置２４に向けて送信されてことが分かる。また、発信者装置２０が受けた電子メールの送信内容１０８は、仲介者装置２２から受信者装置２４に向けて送信された送信内容１０４と同じものである。この送信内容１０８は、仲介者の秘密鍵によって暗号化されたものである。したがって、この送信内容１０８を保持しておくことで、発信者装置２０は、仲介者装置２２によって、電子メールの内容証明に相当するサービスを受けられることになる。

【００５１】図５を参照して、発信者装置２０において実行される処理の流れは以下のようになる。まず、送信すべきメールを作成する（１２０）。このメール自体の内容を秘密にしておくべきであれば（１２２の判断でＹＥＳ）このメールを暗号化する（１２４）。その上で、このメールを内容証明で送るべきか否かを判断し（１２６）、内容証明を用いないときには宛名を受信者にして（１２８）送信する（１３２）。内容証明で送るときには、宛名を仲介者に、転送先を受信者に、それぞれ指定して（１３０）、メールを送信する（１３２）。これで発信時における発信者側装置の処理は終了である。

【００５２】図６を参照して、仲介者装置２２における処理は以下のとおりである。まず、電子メールを受信する（１４０）。この電子メールから転送先の宛名を取り出し（１４２）、発信者の宛名を取り出す（１４４）。次に送信されてきた電子メール本文に、受け取った日付けを追加し（１４６）、さらに仲介者名を追加（１４８）する。次に、この電子メール全体を仲介者自身の秘密鍵４４（図１を参照）で暗号化する（１５０）。

【００５３】次に、転送先が複数あるか否かをチェックする（１５２）。転送先がひとつだけであればその転送先に発信する（１５４）。転送先が複数個あれば、そのすべてに対してこの電子メールを発信する（１５６、１５８）。

【００５４】このようにして行なった電子メールの発信処理の結果、送信エラーがあったか否かを判定する（１６０）。送信エラーがあれば、発信者に対して転送エラー情報を発信する（１６２）。

【００５５】最後に、ステップ１５４またはステップ１５６で転送先に発信したものと同じ電子メールを発信者に対しても送信する（１６４）。以上で仲介者装置で行なわれる処理は終了である。

【００５６】受信者装置では、電子メールの受信時に以下のような処理が行なわれる。図７を参照して、まず電子メールを受信する（１７０）。受信した電子メールの送信者が仲介者装置２２か否かを判定する（１７２）。仲介者からのメールでない場合には処理はステップ１７６に進む。仲介者からのメールであればこの電子メールが内容証明のメールとして送られて来たことを認識し、電子メールの内容を仲介者の公開鍵４６（図１参照）で復号化する（１７４）。

【００５７】次に、ステップ１７６で、電子メールの内容の発信者と発信時間とを確認する。そして、その内容が暗号化されているかどうかを判定する（１７８）。暗号化されていればその内容を復号化する。こうして得られたメールの内容を確認して（１８２）処理を終了する。このようにして、受信者装置では、仲介者装置から送信されてきた電子メールが内容証明のメールであることを知ることができる。

【００５８】一方、発信者装置２０では、図６のステップ１６４で仲介者装置２２から返信されたメールを受け取り以下のような処理を行なう。図８を参照して、発信者装置２０は、電子メールを受け取ると（１９０）、その発信者が仲介者であるか否かを判定する（１９２）。発信者が仲介者でなければ処理はステップ１９８に進む。ステップ１９８以下の処理については後述する。発信者が仲介者であれば、以前に内容証明のメールとして送信したメールが受信者に対して内容証明のメールとして仲介者から発信されたことが分かる。この場合、発信者装置２０は、そのメールを一旦コピーし（１９４）、コピーしたものの内容を仲介者の公開鍵４６（図１参照）を用いて復号化する（１９６）。その後処理はステップ１９８に進む。

【００５９】ステップ１９８では、電子メールの本文が暗号化されているか否かを判定する。本文が暗号化されていればその内容を自己の公開鍵で復号化する（２００）。こうして得られた電子メールの内容につき、その内容が自己が発信した内容と一致するか否かを判定する（２０２）。一致していれば処理が正常に行なわれたと言えるから、メールを保存し（２０４）処理を終了する。一致しなければどこかで問題が生じたということであるから（２０６）、何らかの対応をとる。

【００６０】このような仲介者装置２２を用いた電子メールシステムにより、在来の郵便物における郵便局の内容証明郵便と同様に、どのような内容の電子メールを、いつ、誰に送信したかを証明することができる。また上記したように転送先として複数を指定できるようにしておき、仲介者装置でその複数の転送先の各々に対して内容証明に必要な処理を行なうことにより、発信者は１通の電子メールと複数の宛名とを用意し発信するだけで、同じ内容の複数の電子メールを、異なる宛先に内容証明のメールとして発信させることができる。

【００６１】また上記した実施の形態のシステムでは、受信者に対して送信したのと同一内容の電子メールを仲介者装置から発信者に対して返送している。こうするこ

とで、発信者は自己の電子メールが内容証明のメールとして受信者に対して発信されたことが分かるが、その内容が仲介者の秘密鍵で暗号化されていることから、そのメールが確かに仲介者装置によって発信されたものであることを証明できる。同じ内容の電子メールが受信者に対して発信されたことは仲介者において証明できるから、結局、発信者から受信者に対して送信された電子メールの内容が、仲介者から発信者に対して返送された電子メールの内容と同一であることが証明できることになる。またこの場合、仲介者装置としては、内容証明した電子メールを発信者に対して返送すればよく、内容証明のために自己にそのコピーを保存する必要がない。そのため、仲介者装置にデータを蓄積する必要がなくなり、多数のメールを処理した場合でも外部記憶装置などの資源の不足が生ずるということはない。

【００６２】また、仲介者装置から発信する際に何らかの送信エラーがあった場合、仲介者装置から発信者に対して送信エラー情報が送信される。そのため、たとえばメールサーバ等に故障があって電子メールの送付が正常に行なえなかった場合、発信者がそうした異常を知ることができ、適切な処理をとることが可能である。

【００６３】本願発明にかかる装置および方法を、一実施の形態のシステムに基づいて説明してきたが、本願発明の技術的範囲が上述した実施の形態のシステムに限定されないことはもちろんであり、上記以外にも様々な修正をして実施することができる。

【図面の簡単な説明】

【図１】図１は、本願発明の一実施の形態にかかる電子メールシステムの全体構成を示す模式図である。

【図２】図２は、本願発明の一実施の形態にかかる電子メールシステムで用いられる送信者装置のブロック図である。

【図３】図３は、本願発明の一実施の形態にかかる電子メールシステムで用いられる、仲介者装置のブロック図である。

【図４】図４は、本願発明の一実施の形態にかかる電子メールシステムにおける電子メールのデータの流れを示す模式図である。

【図５】図５は、本願発明の一実施の形態にかかる電子メールシステムにおいて用いられる送信者装置の、メールの送信時のプログラム処理のフローチャートである。

【図６】図６は、本願発明の一実施の形態にかかる電子メールシステムにおいて用いられる仲介者装置のプログラム処理のフローチャートである。

【図７】図７は、本願発明の一実施の形態にかかる電子メールシステムにおいて用いられる受信者装置の、メールの受信時のプログラム処理のフローチャートである。

【図８】図８は、本願発明の一実施の形態にかかる電子メールシステムにおいて用いられる送信者装置の、仲介者装置からのメールの受信時のプログラム処理のフローチャートである。

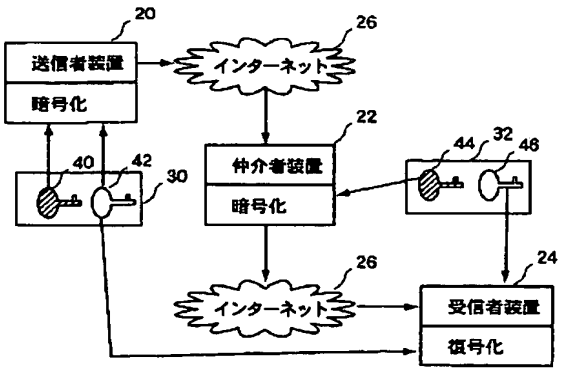
【図９】図９は、従来の電子メールシステムにおける公開鍵システムの使用法を示す模式図である。

【図１０】図１０は、従来の電子メールシステムにおける公開鍵システムの他の使用法を示す模式図である。

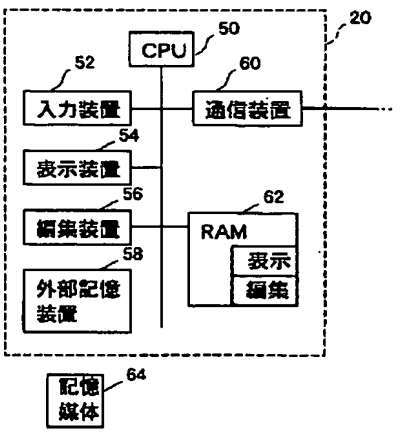
【符号の説明】

２０　送信者装置
２２　仲介者装置
２４　受信者装置
２６　インターネット
５０、７０　ＣＰＵ
６０　通信装置
５８、７８　外部記憶装置
６２、８６　ＲＡＭ
６４、９０　記憶媒体

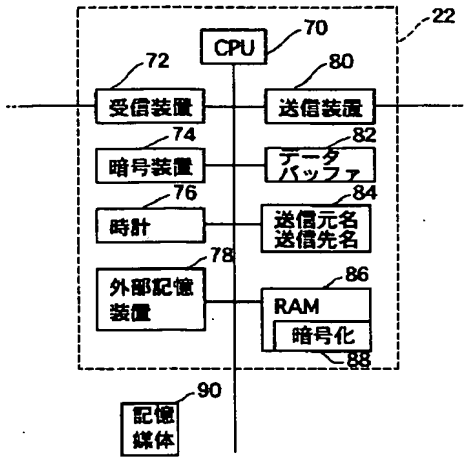
【図１】



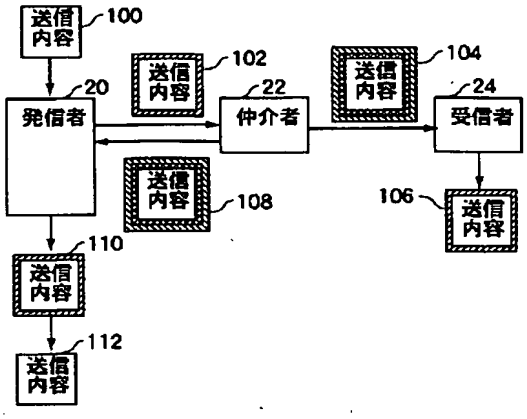
【図２】



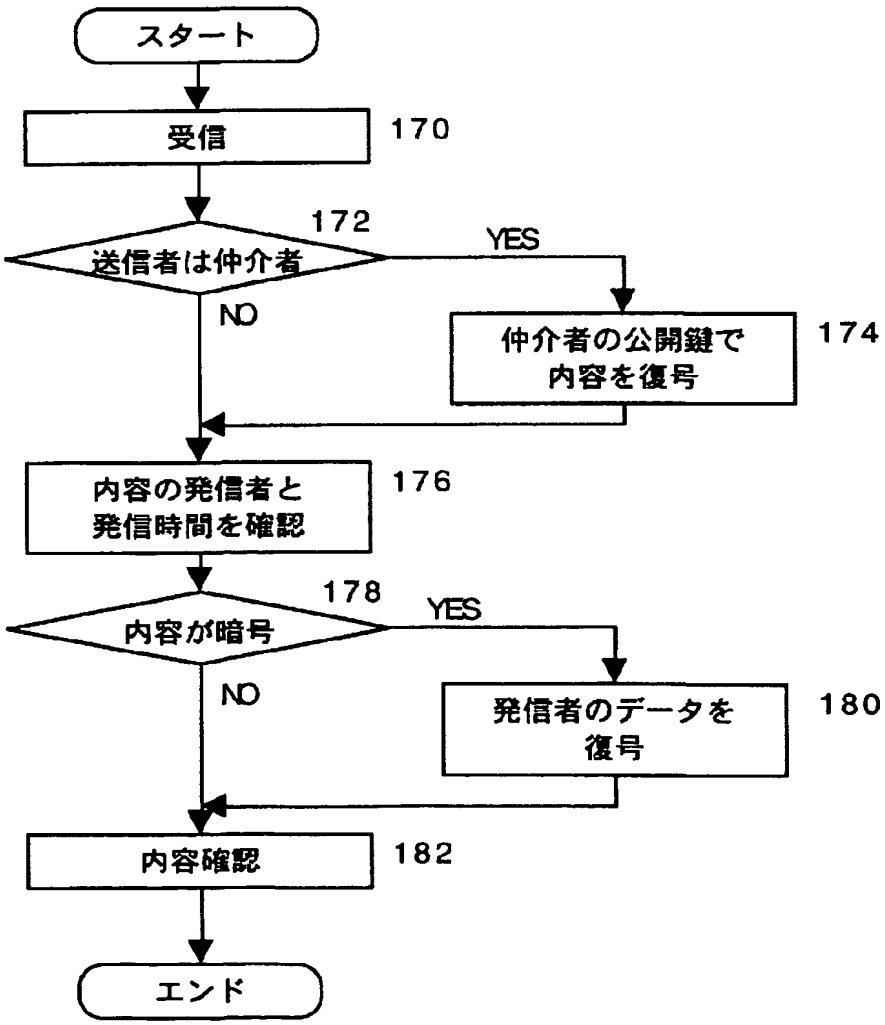
【図３】


22
CPU
70
72
80
受信装置
送信装置
74
82
暗号装置
データバッファ
76
84
時計
送信元名
送信先名
78
86
外部記憶装置
RAM
暗号化
88
90
記憶媒体

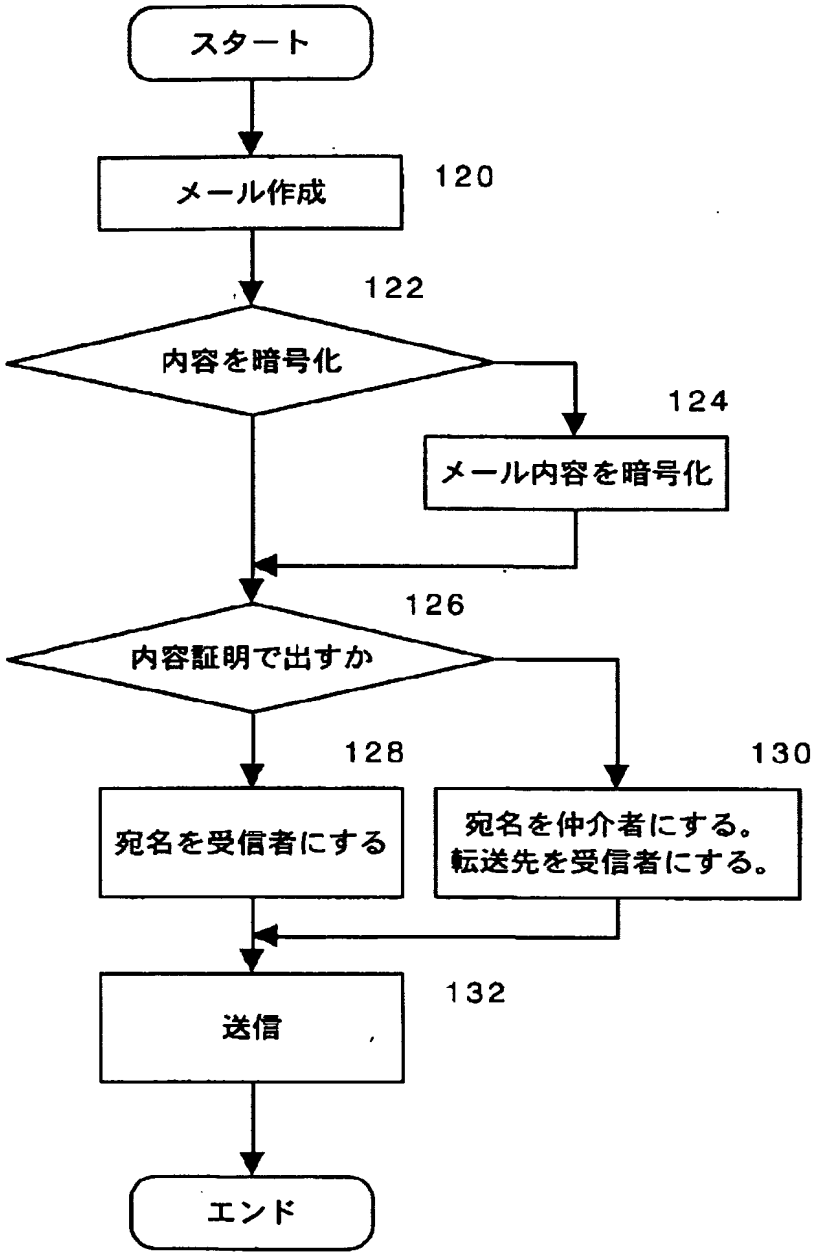
【図４】


送信内容
100
送信内容
102
送信内容
104
20
22
24
発信者
仲介者
受信者
送信内容
108
106
送信内容
110
送信内容
112
送信内容

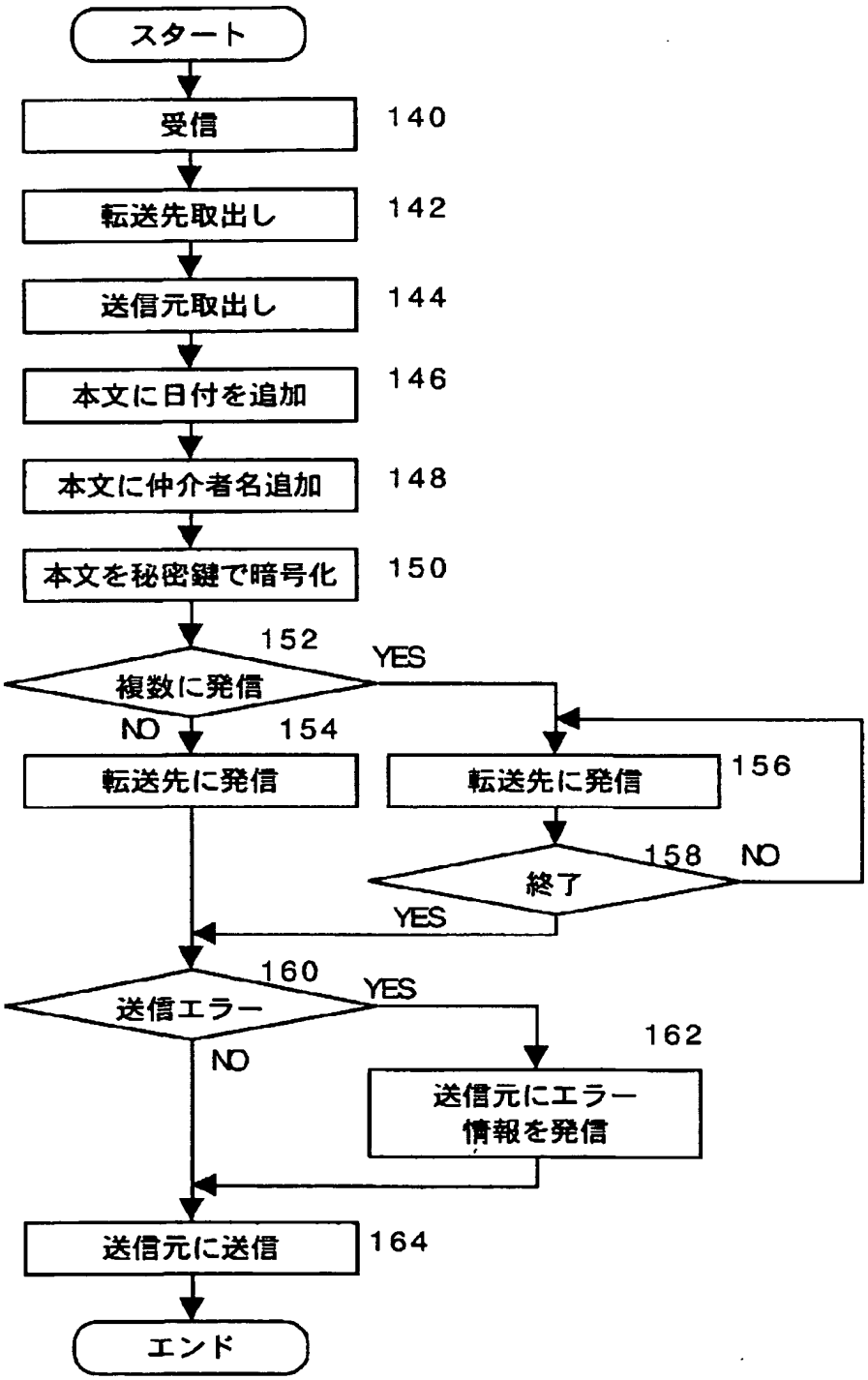
【図７】


スタート
受信
170
172
送信者は仲介者
YES
NO
仲介者の公開鍵で内容を復号
174
内容の発信者と発信時間を確認
176
178
内容が暗号
YES
NO
発信者のデータを復号
180
内容確認
182
エンド

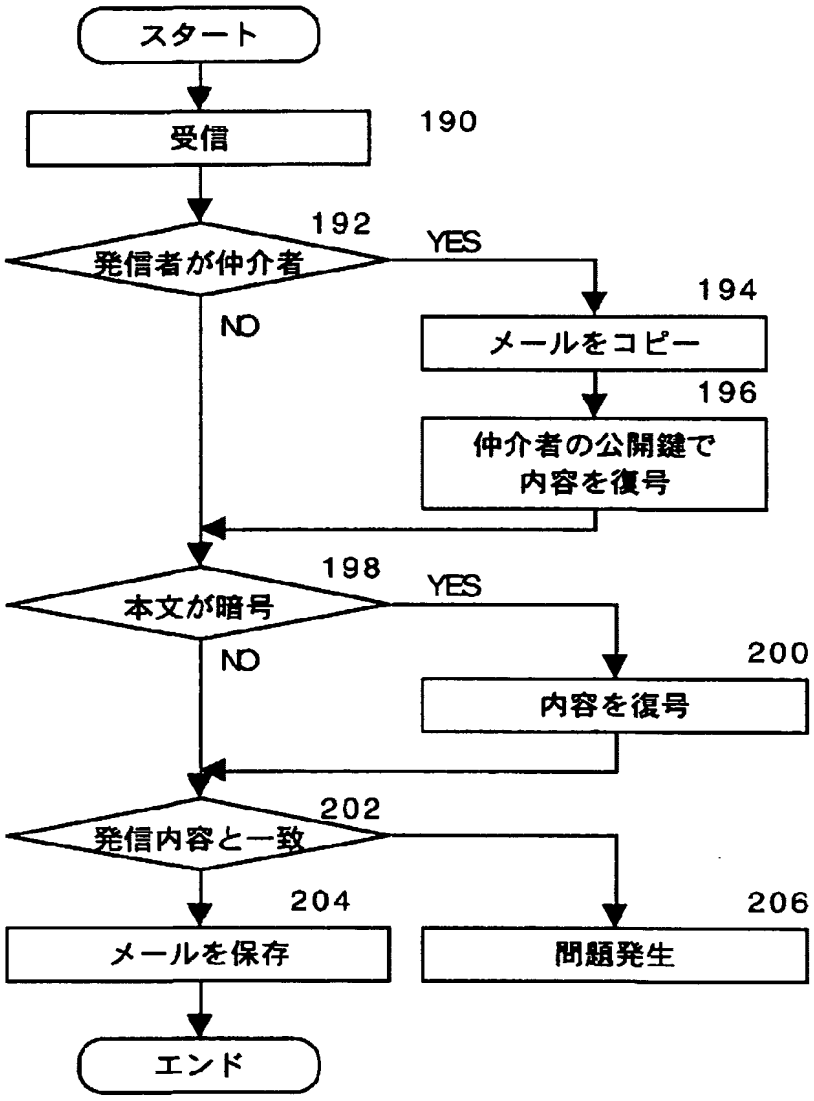
【図５】


スタート
メール作成
120
122
内容を暗号化
124
メール内容を暗号化
126
内容証明で出すか
128
130
宛名を受信者にする
宛名を仲介者にする。
転送先を受信者にする。
送信
132
エンド

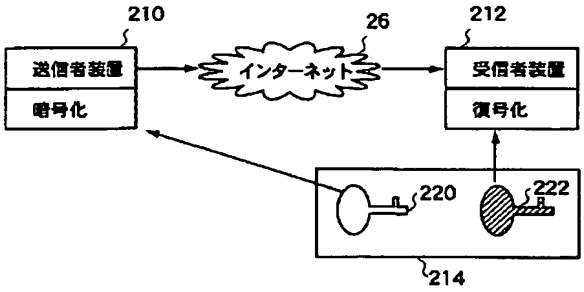
【図６】


スタート
受信
140
転送先取出し
142
送信元取出し
144
本文に日付を追加
146
本文に仲介者名追加
148
本文を秘密鍵で暗号化
150
152
複数に発信
YES
NO
154
転送先に発信
転送先に発信
156
158
終了
NO
YES
160
送信エラー
YES
NO
162
送信元にエラー情報を発信
送信元に送信
164
エンド

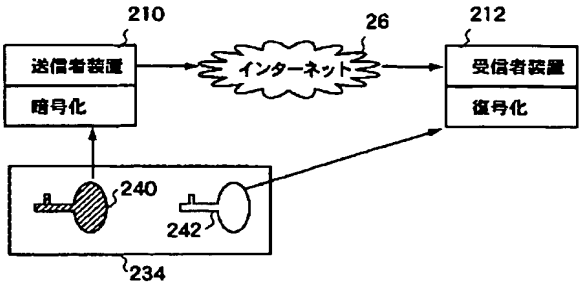
【図８】


スタート
受信
190
192
発信者が仲介者
YES
NO
194
メールをコピー
196
仲介者の公開鍵で
内容を復号
198
本文が暗号
YES
NO
200
内容を復号
202
発信内容と一致
204
メールを保存
206
問題発生
エンド

【図９】


210
送信者装置
暗号化
26
インターネット
212
受信者装置
復号化
220
222
214

【図１０】


210
送信者装置
暗号化
26
インターネット
212
受信者装置
復号化
240
242
234